Implementasi Pengamanan Basis Data dengan Teknik Enkripsi

Andi Irmayana, Komang Aryasa
STMIK Dipanegara Makassar
Jalan Perintis Kemerdekaan Km. 9 Makassar, Telp. (0411) 587194 – Fax. (0411) 588284
e-mail : **andi.irmayana@yahoo.com**, aryuh09@gmail.com

Abstrak

Penelitian ini bertujuan untuk merancang suatu sistem Implementasi Pengamanan Basis Data dengan Teknik Enkripsi yang dapat memberikan keamanan data base dari pengguna yang tidak bertanggungjawab.Penelitian ini menggunakan metode survei dalam mengumpulkan data dan metode eksperimen menggunakan bahasa pemrograman Microsof Visual Basic 6.0dalam merancang sistem dan aplikasi Microsoft Accees dalam mengolah data. Sistem telah diuji menggunakan metode whitebox dimana diperoleh nilai Region, Independen Path dan Cyclomatic Complexcity adalah sama. Oleh karena itu, dapat diambil kesimpulan bahwa aplikasi yang dirancang dapat dikatakan berhasil.

Kata Kunci : Sistem informasi, Enkripsi, Simeteris. Visual Basic 6.0

Abstract

This research aims to design a system with the implementation of Security Database Encryption techniques that can provide security data base of users who are not responsible . This study used a survey method in collecting data and experimental methods using the programming language Visual Basic 6.0 Microsof in designing the system and Microsoft applications Accees in data processing . The system has been tested using whitebox method in which the obtained value Region , the Independent Path and Cyclomatic Complexcity are the same . Therefore , it can be concluded that the application designed was successful

.

Keywords : information systems , encryption , Simeteris, Visual Basic 6.0

1. Pendahuluan

Saat ini, keamanan terhadap data yang tersimpan dalam basis data sudah menjadi persyaratan mutlak. Pengamanan terhadap jaringan komputer yang terhubung dengan basis data sudah tidak lagi menjamin keamanan data karena kebocoran data dapat disebabkan oleh “orang dalam” atau pihak–pihak yang langsung berhubungan dengan basis data seperti administrator basis data. Hal ini menyebabkan pengguna basis data harus menemukan cara untuk mengamankan data tanpa campur tangan administrator basis data.

Kriptografi dapat digunakan untuk mengamankan data. Oleh karena itu, pengguna basis data membutuhkan bantuan untuk memenuhi kebutuhan keamanan akan data yang disimpannya. Penerapan kriptografi pada Tugas Akhir ini akan difokuskan bagaimana kriptografi dapat mengamankan data sampai pada level baris (*row*) dan kolom (*field*) dengan tetap memperhatikan integritas data dan kewenangan setiap pengguna basis data. Algoritma kriptografi yang akan digunakan ialah algoritma kriptografi simetris dan bersifat *stream cipher* sehingga data hasil enkripsi (cipherteks) mempunyai ukuran yang sama dengan data asli (plainteks). Teknik kriptografi simetris dipilih karena diharapkan dengan algoritma ini proses enkripsi-dekripsi data dapat dilakukan dengan waktu yang lebih cepat dibandingkan denganalgoritma kriptografi kunci publik (asimetris) [1].

2. Bahan dan Metode

2.1 Mekanisme Kriptografi

Dalam era teknologi informasi sekarang ini, mekanisme yang sama masih digunakan tetapi tentunya implementasi sistemnya berbeda. Sebelum membahas lebih jauh mekanisme kriptografi modern, berikut ini diberikan beberapa istilah yang umum digunakan dalam pembahasan kriptografi [2][3].

a. *Plaintext*
   Plaintext (message) merupakan pesan asli yang ingin dikirimkan dan dijaga keamanannya. Pesan ini tidak lain dari informasi tersebut.
b. *Chipertext*

***Chipertext* merupakan pesan yang telah dikodekan (disandikan) sehingga siap untuk dikirimkan.**

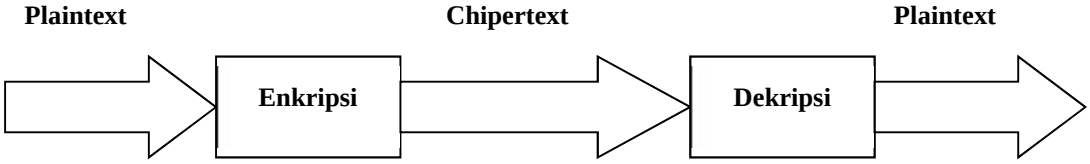
c. *Chiper*
Chiper merupakan algoritma matematis yang digunakan untuk proses penyandian plaintext menjadi ciphertext.

d. *Enkripsi*
Enkripsi (*encryption*) merupakan proses yang dilakukan untuk menyandikan plaintext sehingga menjadi chipertext.

e. *Dekripsi*
Dekripsi (*decryption*) merupakan proses yang dilakukan untuk memperoleh kembali plaintext dari chipertext.

f. *Kriptosistem*
Kriptosistem merupakan sistem yang dirancang untuk mengamankan suatu sistem informasi dengan memanfaatkan kriptografi.

Urutan-urutan proses kriptografi dapat digambarkan sebagai berikut.



Gambar 1. Mekanisme kriptografi

Prosesnya pada dasarnya sangat sederhana. Sebuah plaintext (m) akan dilewatkan pada proses enkripsi (E) sehingga menghasilkan suatu ciphertext (c). Kemudian untuk memperoleh kembali plaintext, maka ciphertext (c) melalui proses dekripsi (D) yang akan menghasilkan kembali plaintext (m).

2.2 Kriptografi dan Sistem Informasi

Keamanan telah menjadi aspek yang sangat penting dari suatu sistem informasi.Sebuah informasi umumnya hanya ditujukan bagi segolongan tertentu.Oleh karena itu sangat penting untuk mencegahnya jatuh kepada pihak-pihak lain yang tidak berkepentingan.Untuk melaksanakan tujuan tersebutlah dirancang suatu sistem keamanan yang berfungsi melindungi sistem informasi.

Salah satu upaya pengamanan sistem informasi yang dapat dilakukan adalah kriptografi. Kriptografi sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi, antara lain seperti kerahasiaan, integritas data, otentikasi, dan ketiadaan penyangkalan [4].

2.3 Kriptografi Simetrik

Kriptografi simetrik (*symmetric cryptography*) atau dikenal pula sebagai kriptografi kunci rahasia (*secret-key cryptography*), merupakan kriptografi yang menggunakan kunci yang sama baik untuk proses enkripsi maupun dekripsi. Secara matematis dapat dinyatakan bahwa [5]:

$$e = d = k$$

$$E_k(m) = c$$

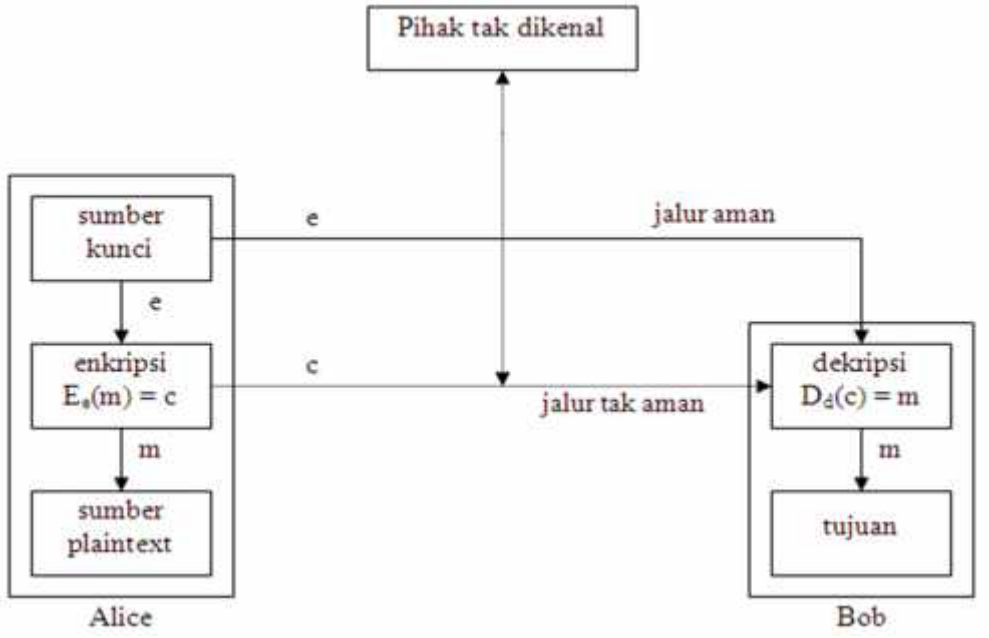
$$D_k(c) = m$$

Kriptografi simetrik sangat menekankan pada kerahasiaan kunci yang digunakan untuk proses enkripsi dan dekripsi. Oleh karena itulah kriptografi ini dinamakan pula sebagai kriptografi kunci rahasia.

Mekanisme kerja kriptografi simetrik antara dua pelaku sistem informasi, Alice dan Bob, adalah sebagai berikut [6][7],

1. Alice dan Bob menyetujui algoritma simetrik yang akan digunakan.
2. Alice dan Bob menyetujui kunci yang akan dipakai.
3. Alice membuat pesan plaintext yang akan dikirimkan kepada Bob, lalu melakukan proses enkripsi dengan menggunakan kunci dan algoritma yang telah disepakati sehingga menghasilkan ciphertext.
4. Alice mengirimkan ciphertext tersebut kepada Bob.

5. Bob menerima ciphertext, lalu melakukan dekripsi dengan menggunakan kunci dan algoritma yang sama sehingga dapat memperoleh plaintext tersebut.



Gambar 2.Mekanisme kriptografi simetrik

Dari gambar 2 dapat dilihat bahwa harus ada jalur aman (*secure channel*) dahulu yang memungkinkan Bob dan Alice melakukan transaksi kunci. Hal ini menjadi masalah karena jika jalur itu memang ada, tentunya kriptografi tidak diperlukan lagi dalam hal ini.Masalah ini dikenal sebagai masalah persebaran kunci (*key distribution problem*).Kelemahan lainnya adalah bahwa untuk tiap pasang pelaku sistem informasi diperlukan sebuah kunci yang berbeda. Dengan demikian bila terdapat n pelaku sistem informasi, maka agar tiap pasang dapat melakukan komunikasi diperlukan kunci sejumlah total n (n – 1) / 2 kunci. Untuk jumlah n yang sangat besar, penyediaan kunci ini akan menjadi masalah, yang dikenal sebagai masalah manajemen kunci (*key management problem*). Namun di samping kelemahan tersebut, kriptografi simetrik memiliki keuntungan juga.Keuntungan menggunakan kriptografi simetrik ini adalah kecepatan operasinya yang sangat baik.Dibandingkan dengan kriptografi asimetrik, kriptografi simetrik memiliki kecepatan operasi yang jauh lebih cepat.

3. Metode Perancangan

3.1. Peralatan

1. Perangkat keras yang digunakan, yaitu:
    1. Laptop Asus K42F
    2. Processor Intel Core I3-50 4 2,8 GHz
    3. Memory 4GB
    4. Harddisk 500 GB

2. Perangkat Lunak yang digunakan, yaitu:
    1. Bahasa pemograman Visual Basic 6.0
    2. Sistem operasi Windows XP

3. Perangkat Konseptual :
    1. Diagaram Alir Sistem

3.2 Tahapan Perancangan

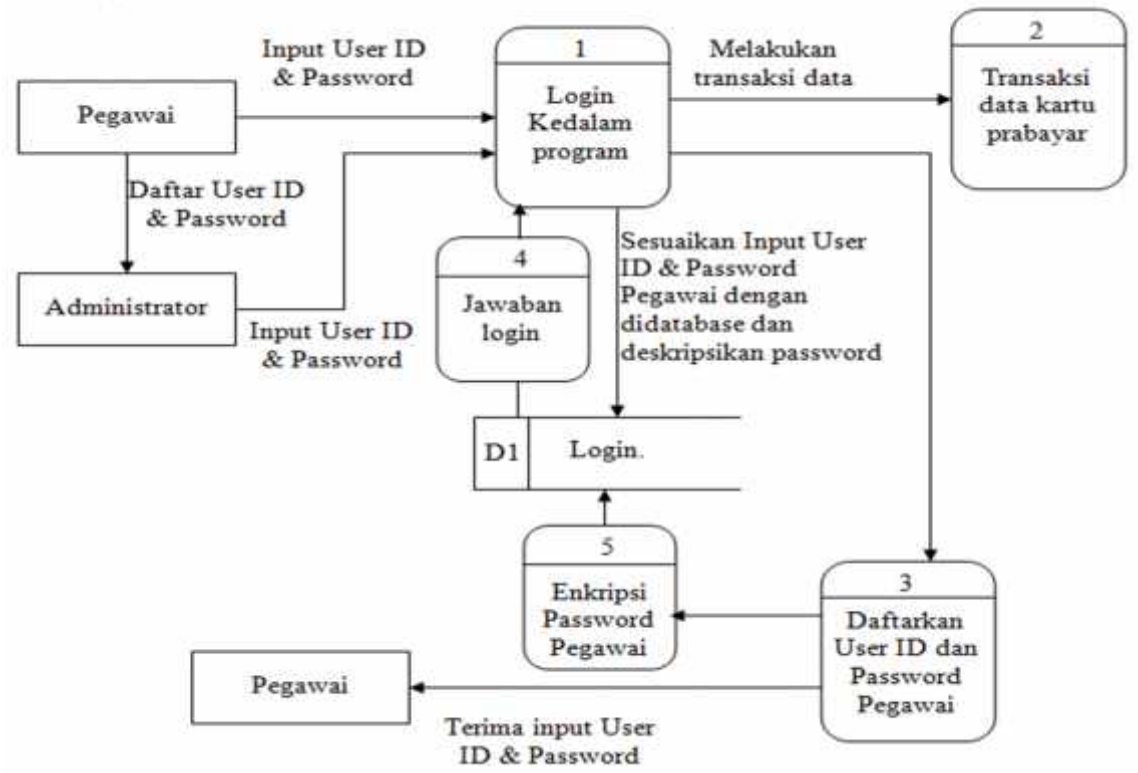
Tahapan perancangan dilaksanakan sebagai berikut :

1. Studi Literatur, yaitu dengan melakukan studi dari buku-buku pustaka yang berkaitan dengan masalah yang dibahas, juga melalui artikel-artikel dari internet.
2. Observasi dan wawancara langsung.

3. Mengumpulkan data yang diperoleh melalui dokumen-dokumen dan buku-buku paket lainnya yang relevan dengan masalah yang akan diteliti..
4. Membuat Perancangan Sistem berupa Diagram kontes, rancangan kamus data, rancangan input dan output.
5. Merancang sistem mengunakan bahasa pemrograman visual basic 6.0 dan membangun database menggunakan mysql.
6. Implementasi dan Pengujian sistem menggunakan Metode white box
7. Menarik kesimpulan dan memberikan saran-saran yang dianggap perlu.

3.4 Rancangan Sistem

3.4.1. Diagram Aliran



Gambar 3.Diagram Alir

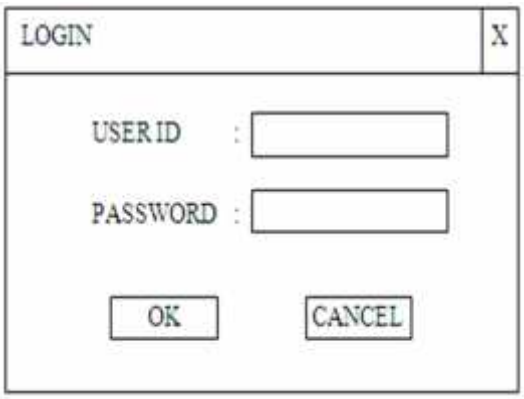
Terlihat pada gambar diatas setiap pengguna/pegawai yang akan melakukan kegiatan menggunakan sistem informasi kartu harus melakukan input user id dan password. Setelah user id dan password program otomatis akan mengecek apakah user id dan password terdapat didalam database dan mencocokkannya. Saat pengguna selesai mengisi user id dan password dan mengenter ok otomatis program akan mendeskripsikan password didalam database. Jika user id dan password cocok maka pengguna dapat menggunakan program sistem informasi kartu dan jika tidak cocok maka pengguna diharuskan mengulang pengisian user id dan password.

Dan bagi pengguna yang belum memiliki user id dan password harus menghubungi super admin atau meminta kepada yang sudah memiliki user id dan password untuk mendaftarkan user id dan passwordnya kedalam database.Untuk mendaftar dan mengubah password digunakan menu user account. Pada saat pendaftaran user id dan password program otomatis akan mengenkripsikan password kedalam bentuk enkripsi didalam database login.

3.4.2. Rancangan Program Enkripsi

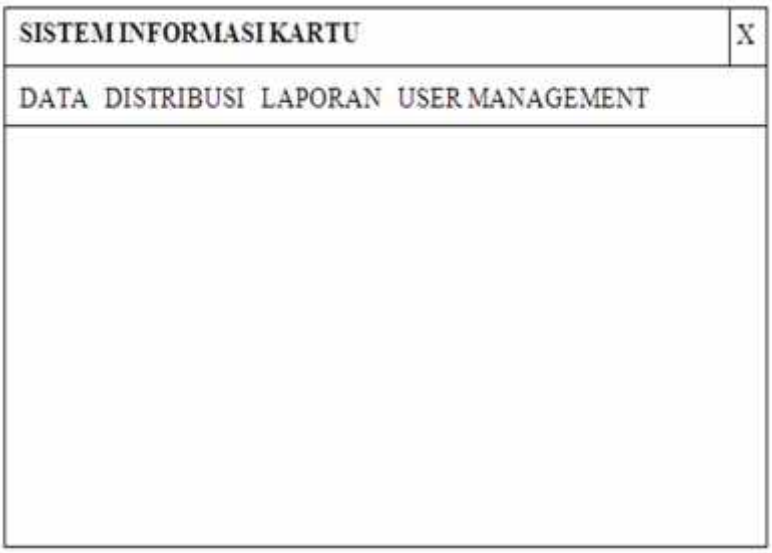
Perancangan program enkripsi ini digunakan untuk membantu pengamanan database login pada program sistem informasi kartu.

a. Perancangan Form



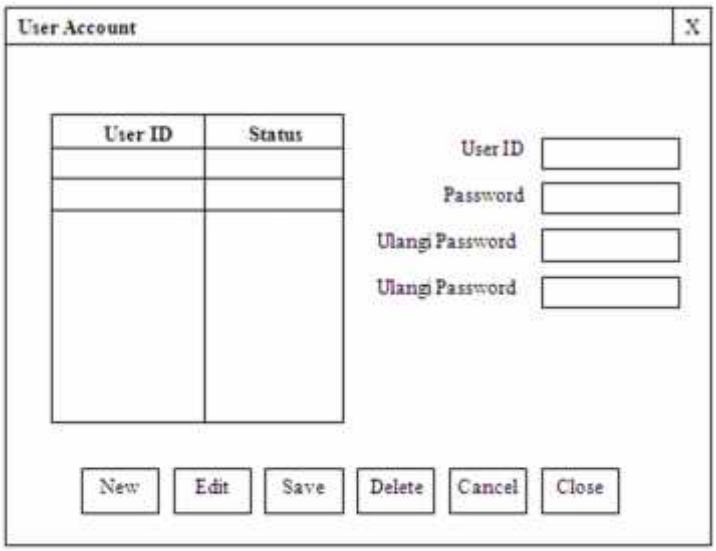
Gambar .4. Perancangan form login

Sebelum masuk kedalam program terdapat menu yang pertama yaitu menu login. Jadi setiap pengguna yang akan menggunakan program sistem informasi kartu ini harus melakukan login. Dalam menu login ini pengguna harus mengisikan user id dan password



Gambar5. Perancangan menu utama sistem informasi kartu

Form menu utama merupakan induk dimana penginputan data, transaksi-transaksi serta laporan-laporan diletakkan disini (dimulai dari sini).

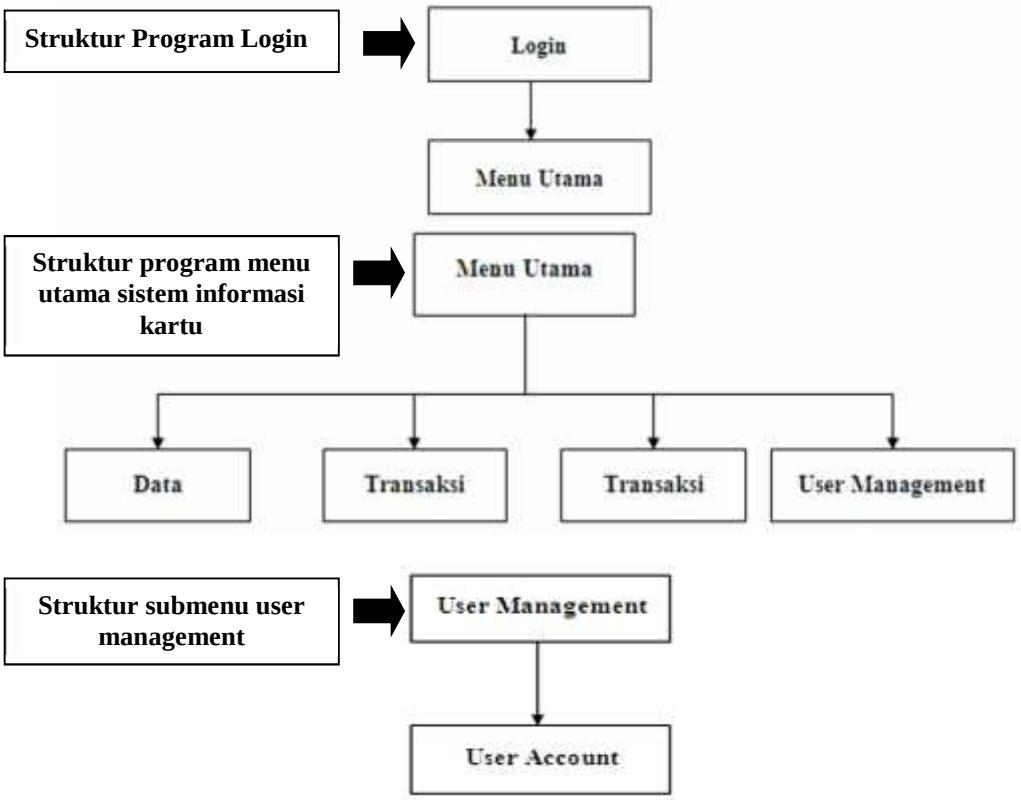


Gambar 6. Perancangan form user account

Pada menu user account ini digunakan untuk mendaftarkan pengguna yang akan menggunakan program sistem informasi kartu dan bila pengguna yang ingin mengganti password yang lama

b. Perancangan Struktur Program

Adapun struktur program dari program sistem informasi kartu adalah sebagai berikut :



Gambar 7. Perancangan struktur program

4. Hasil dan Pembahasan

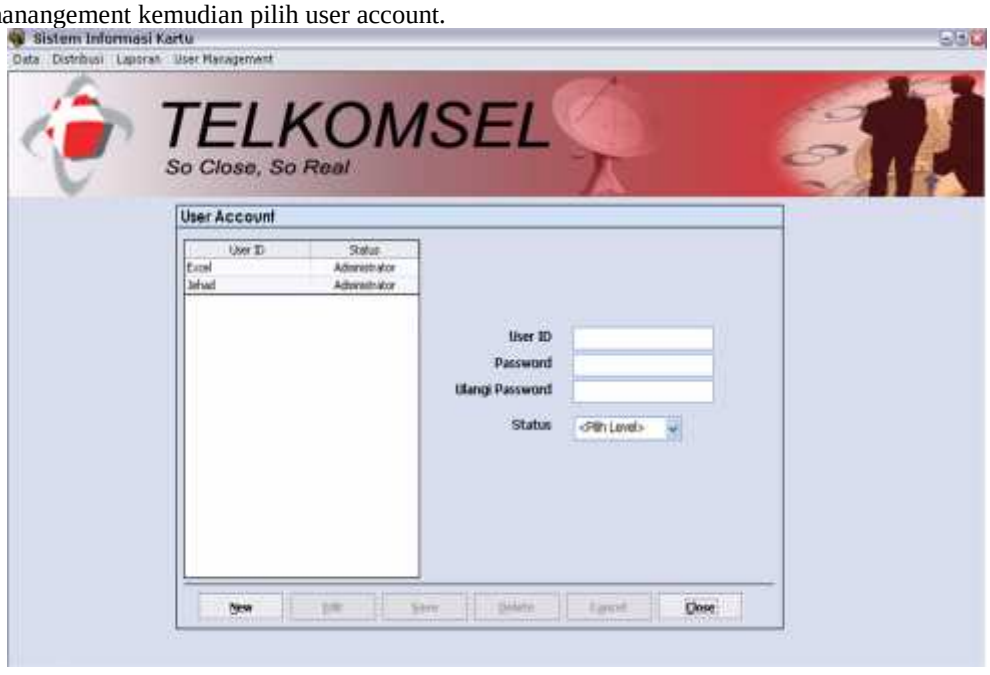
Untuk dapat masuk ke dalam menu program sistem informasi kartu setiap pengguna harus melakukan login program dengan memasukkan User ID dan Password bila User ID dan Password sudah terdaftar dan sesuai dengan yang ada didatabase maka program sistem informasi kartu dapat terbuka (digunakan). Jika User ID dan Password tidak terdaftar dan salah maka program sistem informasi kartu tidak dapat digunakan (terbuka).Terlihat pada gambar berikut menu login untuk masuk ke dalam program sistem informasi kartu.

Gambar 8. Menu login

Untuk melakukan login pengguna harus memasukkan User ID selanjutnya memasukkan passwordnya kemudian tekan login.Dan bila pengisian User ID dan Password anda ada yang salah dapat menekan tombol batal.Setelah tombol login ditekan dan User ID dan password sesuai dengan didatabase maka pengguna dapat melihat menu utama program sistem informasi kartu seperti pada gambar 9.berikut.

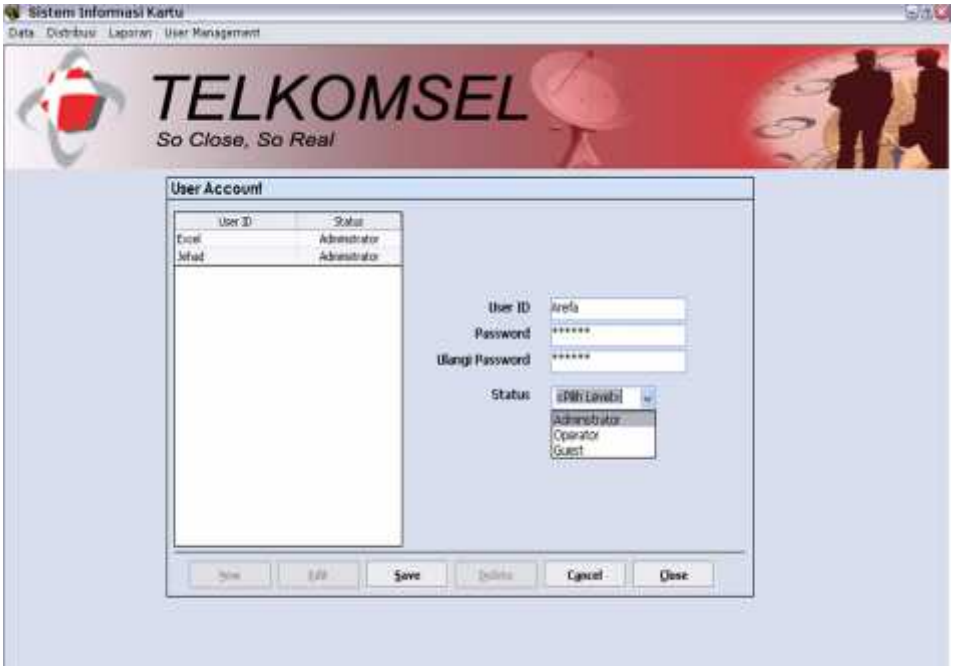
Gambar 9. Menu utama program

Bagi pengguna yang ingin mendaftar atau mengubah password lamanya dapat menggunakan user manangement kemudian pilih user account.



Gambar 10. Menu user account

Setelah masuk kedalam menu user account.Bagi pengguna yang mendaftar dapat mengklik tombol new kemudian isikan User ID dan Password dan isi ulang Password dan pilih statusnya.Pada gambar 11.ditampilkan contoh pengisian user account yang baru.



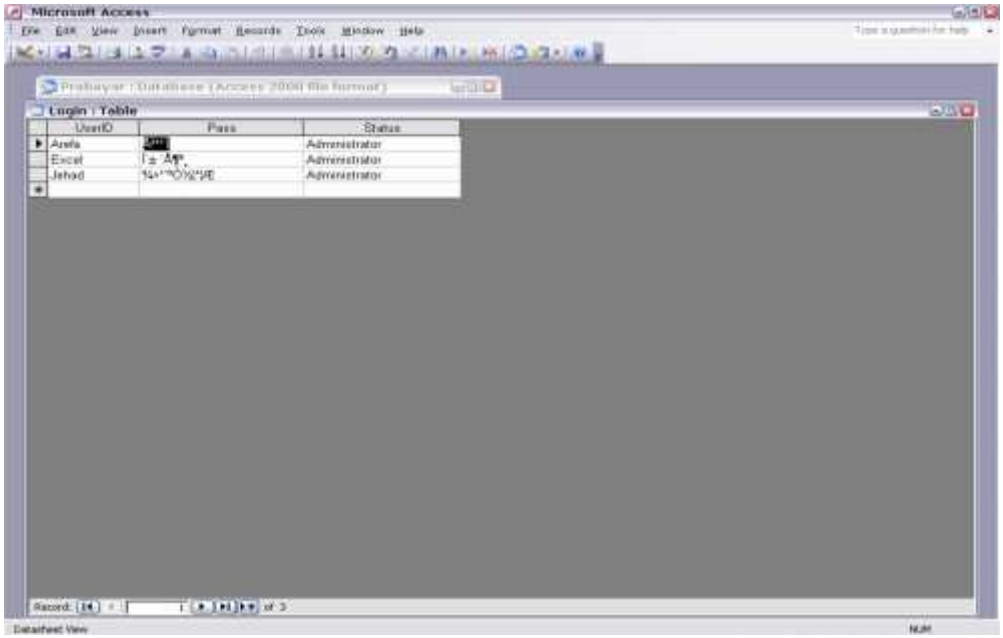
Gambar 11. Tampilan pengisian user account

Setelah seluruh inputan diisi maka dilanjutkan untuk menyimpan atau bila anda ada merasa ragu dengan User ID ataupun pengisian password dan ulangi password ataupun salah dalam memilih status dapat menekan tombol cancel. Dan untuk keluar dari program user account dapat mengklik tombol close.

Gambar 12. Bentuk pengisian user account

Setelah data-data yang harus diisi telah penulis isi dan penulis telah menyimpannya maka data penulis tampak pada tabel user id didalam user account dimana ditampilkan pada tabel tersebut seluruh pengguna yang telah terdaftar dengan statusnya.

Selanjutnya kita dapat melihat bentuk basisdata pengenkripsian dari pengisian data-data pada menu user account pada tabel database login seperti yang ditunjukkan pada gambar 12 berikut.



Gambar 13. Tabel database login

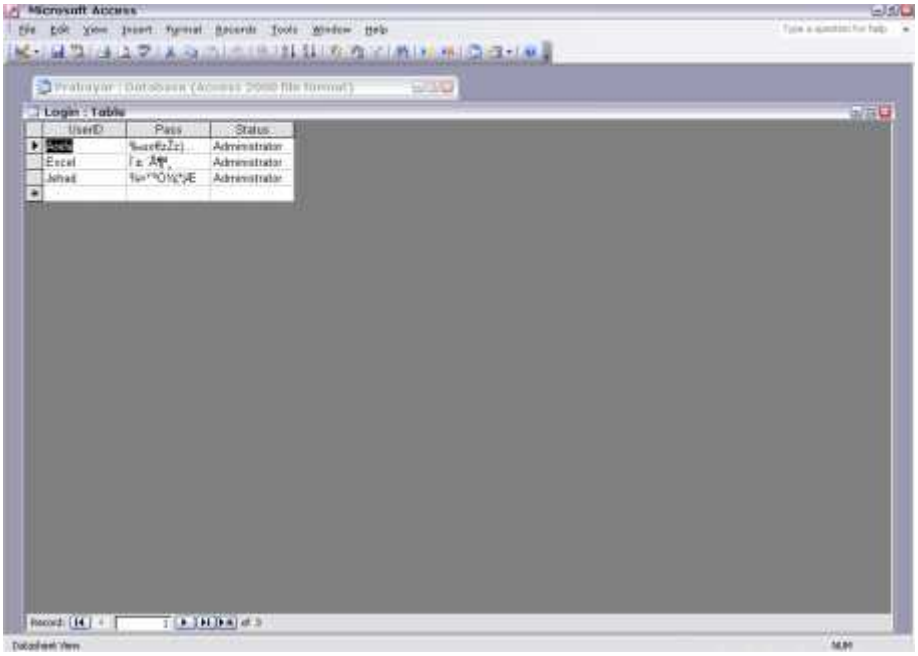
Pada gambar 13 terlihat bentuk pengenkripsian daripada database dimana yang dienkripsi adalah data password dari user id. Dengan pengenkripsian tersebut seseorang yang ingin menggunakan program sistem informasi kartu tidak dapat menggunakan user id yang lain untuk masuk ke dalam program sistem informasi kartu karena data passwordnya telah terenkripsi.

Gambar 14. Penggantian password lama

Disini penulis mencoba untuk mengganti password lamanya dengan password baru.Dalam pergantian password ini pengguna harus mengisi data-data User ID dan password lama serta statusnya.Setelah data-data tersebut diisi maka tekan tombol lanjut.

Setelah tombol lanjut ditekan maka akan muncul pengisian data-data untuk pengisian data-data baru anda seperti halnya pada gambar 14. Setelah data-data baru penulis isi kemudian penulis menyimpannya.

Berikut penulis tampilkan database dari data-data penulis yang baru seperti pada gambar 15 berikut.



Gambar 15. Bentuk database login

5. Kesimpulan

Sistem Implementasi Pengamanan Basis Data dengan Teknik Enkripsi berhasil dirancang menggunakan bahasa pemograman visual basic 6.0 dan Microsoft Access, sehingga dapat digunakan untuk keamanan database dari pengguna yang tidak bertanggungjawab. Sistem telah diuji menggunakan metode whitebox dimana diperoleh nilai Region, Independen Path dan Cyclomatic Complexcity adalah sama. Oleh karena itu, dapat diambil kesimpulan bahwa aplikasi yang dirancang dapat dikatakan berhasil.

Daftar Pustaka

[1] A. Rahmani, *Implementasi Teknik Kriptografi Blowfish untuk Pengamanan Basis Data*, Tesis Magister Departemen Teknik Informatika, ITB, 2003.
[2] A. Silberschatz, H. F. Korth. Dan S. Sudarshan, *Database System Concepts, 4th Edition*, McGraw – Hill, 2002.
[3] B. Schneier, *Applied Cryptography: Protocols,Algorithms, and Source Code in C, 2nd Edition*,John Wiley & Sons, Inc, 1996.
[4] B. Trower, *Crypt Data Packaging*, Trantor Standard Systems Inc.
[5] Fathansyah, *Basis Data*, Informatika, Bandung, 1999.
[6] R. Munir, *Bahan Kuliah IF5054 Kriptografi*, Departemen Teknik Informatika, ITB, 2004.
[7] T. Marcus, A. Prijono dan J.Widiadhi, *DELPHI DEVELOPER dan SQL Server 2000*, Informatika, Bandung, 2004.